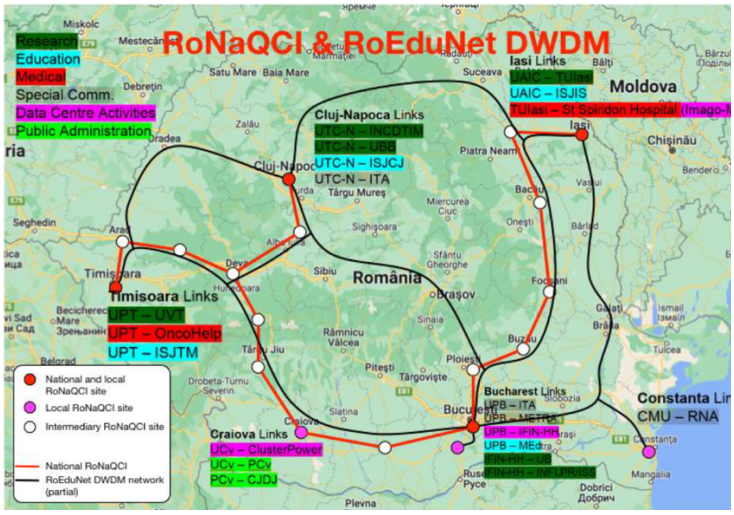
Strategic Move in Global Security: Quantum Software Enhanced by ID Quantique in the Largest QKD Network of EuroQCI

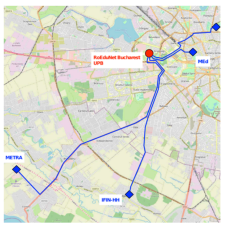
Quantum computers, via Shor's algorithm, are capable of breaking classical encryption such as RSA, elliptic curve cryptography, and more. In the context of rapid advancements in quantum computing technology, the security of modern communication is at severe risk. To this day, the only known key exchange method that is information-theoretically secure (i.e. safe against attackers with unlimited computing power, including quantum computers) is quantum key distribution (QKD).

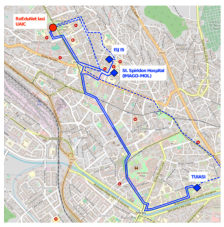
In January 2023 started the implementation phase of European Quantum Communication Infrastructure (EuroQCI), wherein more than 200 million euros were committed by the European Commission and all 27 EU Member States in order to build national QKD networks for secure communication infrastructure in each Member State.

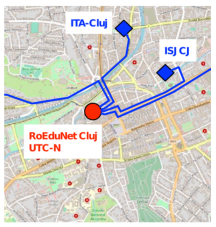
In Romania, the national QKD project under EuroQCI was the **Romanian National Quantum Communication Infrastructure (RoNaQCI)**, an EUR 10M project coordinated by the National University of Science and Technology POLITEHNICA Bucharest partnering with RoEduNet, the Romanian Educational and research Network, which provided the connecting fiber links. The project, largest in EuroQCI, was **based solely on QKD equipment made by ID Quantique**. The project started in January 2023 and was, to our knowledge, **the first EuroQCI project to finalize successfully** in June 2025. From the outset, the project was already expected to have a **significant impact at the EU level**, as per the review from the European Commission: *"The successful implementation of the project will place Romania in a strong position in the area of quantum communication. Apart from the network deployment itself, a particularly valuable element is the staff development plan aimed especially at young specialists and network users. The proposal will ensure the sustainability of the development of quantum technologies in Romania and contribute to the reinforcement of the digital supply chain in the EU."*

RoNaQCI formed in Romania **the largest terrestrial QKD network in EuroQCI**, with **36 total QKD links covering 1500+ km** (amounting to **more than 20% of the QKD network span across EuroQCI**), in **six metropolitan networks** in the cities of Bucharest, Iași, Timișoara, Craiova, Cluj-Napoca, and Constanța, connected by a national QKD backbone and providing secure applications for **special communications, medical data, education, research, data center activities, and more**. The project brought together **12 universities, 7 research institutes, 3 national agencies, 3 private companies, and 5 relevant stakeholders**.



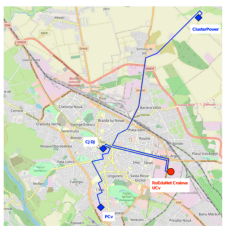

RoNaQCI Bucuresti


RoNaQCI Iasi



RoNaQCI Cluj-Napoca

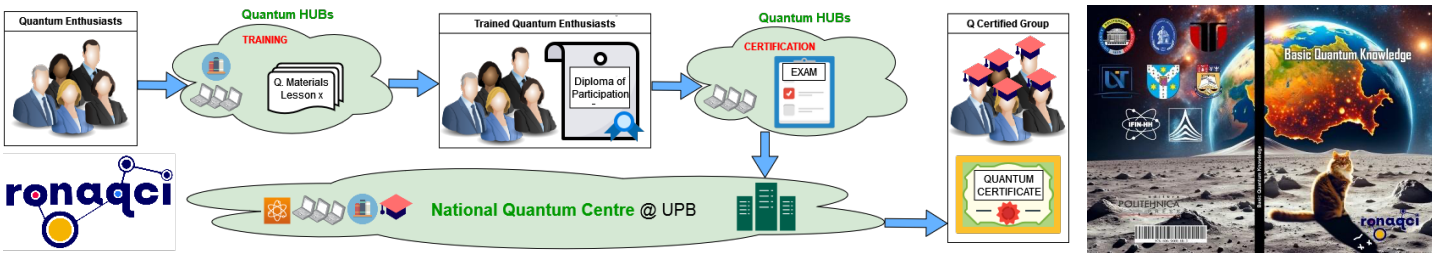

RoNaQCI Timisoara


RoNaQCI Craiova


RoNaQCI Constanta

The impact of RoNaQCI goes far beyond the deployment of the infrastructure. During its operation, RoNaQCI achieved several important milestones. RoNaQCI delivered **practical integration work through software implementations publicly released**: GetKeyTool Infrastructure interface for ETSI GS QKD 014, post-quantum VPN enhanced by QKD, unconditionally secure QKD vaults, libqrng REST API for ID Quantique QRNG, qSSH OpenSSL

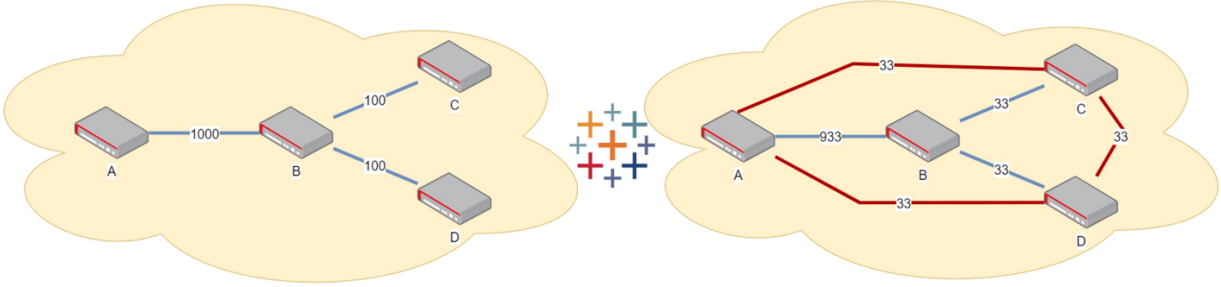
provider implementation, monitoring and operational visibility stack for QKD networks. **The software has been appraised** as: *"the approach aligns with ETSI standards, and [...] it represents a tangible and standards-aligned software solution with clear potential for future exploitation"*.



On the skills and training side, within RoNaQCI, **18 national quantum HUBs** have been established for training and education, with **13 large-scale trainings held**, and **7 national workshops** were organized with a strong educational dimension. Between the workshops and the HUB trainings, **more than 1600 users have been trained** in basic QKD and quantum knowledge, **900+ diplomas of participation have been issued**, and **160+ certifications have been awarded**, using the **certification infrastructure** developed within RoNaQCI and based on the book ***Basic Quantum Knowledge*** authored and published by the consortium.

The **monitoring dashboard solution QKD MonDash,** developed by POLITEHNICA Bucharest, designed specifically to be **fully compatible with ID Quantique devices**, extends the built-in monitoring capacity of QKD networks by collecting QoS data from actual QKD end-user applications, anonymous usage statistics, as well as providing administrators of ID Quantique networks useful overseeing and alarm tools. MonDash was used successfully in conjunction with the deployed RoNaQCI network during the **Romanian QKD national testing day in early August 2025, in which 2442 total keys were exchanged within 12 simultaneous use-cases across 6 different nodes along distances of more than 1000 km on ID Quantique devices**.

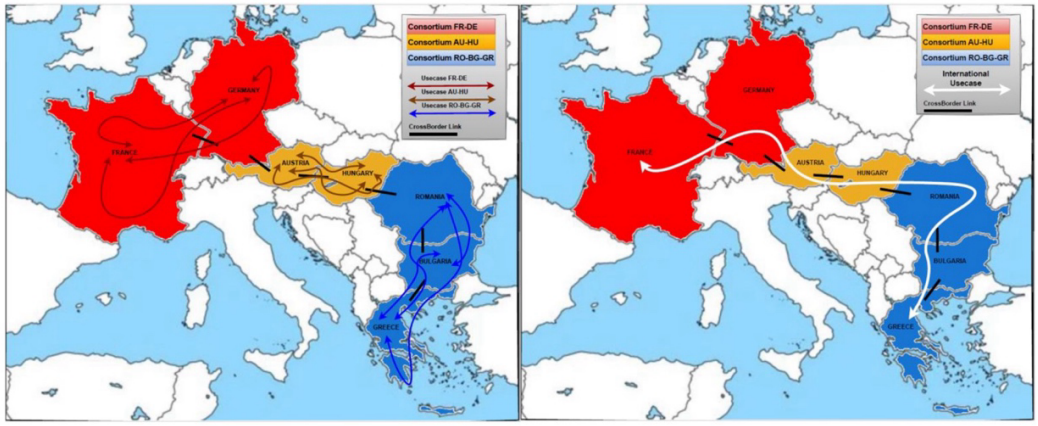
Partially supported by RoNaQCI, the "*Optimal key forwarding strategy in QKD behaviours*" paper has been published in Nature Scientific Reports, **describing for the first time the expected behaviors of large QKD networks**, and providing **optimal key distribution strategies that have been successfully implemented on ID Quantique devices** in POLITEHNICA Bucharest.



Research performed by Prof. P.G.Popescu and Dr. A.B.Popa at POLITEHNICA Bucharest, partially supported by RoNaQCI, has led to the creation of the **international policy for EuroQCI scalability, endorsed by the EC, HaDEA,**

and PETRUS, disseminated to 25 EU Member States and impacting more than 19 CEF EuroQCI applicant consortia which added dedicated tasks or work packages towards the scalability solutions recommended in POLITEHNICA Bucharest's policy.

Preparing for the CEF Call
Assessing a major financial risk due to the impossibility of scaling the European QKD Network



Concerns (with examples)

Consider the image above where different consortia link several countries as depicted. An interconsortium usecase is desired between Paris and Athens, even though Greece and France are part of different consortia. Consider the following concerns:

1. Since QKD links have a limited bandwidth and keys can only be used once, if a network uses up all the keys produced for internal use-cases, **no keys will be left for interconsortium usecases**. *Example: assume the Orange consortium (Austria and Hungary) use all available key bandwidth for AT-HU usecases; thus, no keys are left for a Paris-Athens usecase.*
2. If a country has no incentive to provide neighboring countries with access to its QKD network, it **may not be possible politically**. *Example: assume the Orange consortium (AT and HU) do not wish to provide access to Orange keys to the Red and Blue countries; thus, no Paris-Athens usecase will be possible.*
3. There is no mechanism for prioritizing a specific usecase, which is **crucial in crisis or emergency situations**. *Example: consider an emergency diplomatic issue between France and Greece which require total prioritization for all available bandwidth along this path; with the current technology emergency prioritization is impossible to achieve.*
4. If one network becomes compromised, there is **no protocol for damage control, risk mitigation, or temporary solutions**. *Example: consider the network in HU undergoes a cyber attack and becomes compromised; this compromises the communication between all of the western (FR, DE, AT) and eastern (RO, BG, GR) sides, who may not even be aware of the situation.*

Consequence on CEF-DIG-2024-EUROQCI – major operational, financial, and public opinion risks

Due to the concerns above, several of CEF's objectives as highlighted in the call document will be impossible to achieve. Namely:

- The goal of a pan-European collaboration ("*the provision of fibre links between the EuroQCI and a panEuropean network of Security Operation Centres (SOCs)*", "*will ultimately support the growth of a pan-European quantum industry*") – at best, **CEF will lead to a highly segmented QKD network** where usecases are only possible on small groups of 2-3 countries.
- Protecting critical infrastructures between Member States ("*Boost Europe's capacity to protect critical public infrastructures by securing their communications and data, especially those that cross national borders and serve more than one Member State*") – **CEF will not be able to protect critical infrastructures in emergency or cyberattack situations where it is most needed**; moreover, fixing the issue at a later stage may be prohibitively expensive.
- Demonstrating the viability of EuroQCI as a whole ("*expected result is to increase in the number of national QCI networks connected by cross-border terrestrial or satellite links and capable of demonstrating the viability of the EuroQCI as a whole*") – if large interconsortium usecases are not possible, **EuroQCI may be considered a failure both by the national administrations and by the general public**

Recommendation for a simple viable solution

Our recommendation is to add the following paragraph in the CEF call document: "We strongly recommend each project to include in the proposal a plan of action (for example, a software layer) for inter-consortium operational collaboration, covering topics such as key rate bandwidth, network orchestration, protocols for governance and providing access to the proposed cross-border links to an external consortium, external use-case prioritization in emergency situations, protocols for external network breach mitigation."

[0] Popa, Alin-Bogdan, and Pantelimon George Popescu. "Optimal key forwarding strategy in QKD behaviours." *Scientific Reports* 14 (2024).
[1] Popa, Alin-Bogdan, and Pantelimon George Popescu. "The future of qkd networks." *arXiv preprint arXiv:2407.00877* (2024).
[2] Popa, Alin-Bogdan, and Pantelimon Popescu. "CEF: Connecting Elaborate Federal QKD Networks." *arXiv preprint arXiv:2409.12027* (2024).

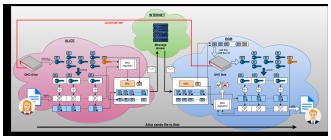
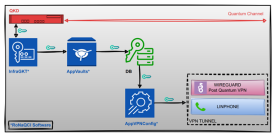
Quantum Team @ National University of Science and Technology POLITEHNICA Bucharest, Romania

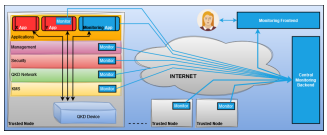
The results achieved within RoNaQCI have translated into new opportunities for Romania and in particular for POLITEHNICA Bucharest, with **four new QKD projects within the second phase of EuroQCI**; worth mentioning are **QRUSOE (the national optical ground station project of France)** and the **Romanian Optical Ground Station (ROGS)**, in which EUR 7.5M have been allocated for the construction of an optical ground station compatible with

the Eagle1 and SAGA missions for secure communication, as well as to **extend the already significant contribution to the European software landscape in quantum-critical areas**: satellite and QKD simulation, scheduling and prediction, optimal QKD key forwarding, and protocols for scalability, governance, and breach mitigation.

1500+ KMs of QKD Links	**36** QKD Links (20 City Links and 16 National Backbone Links)	**1600+** Trained Users, Students, Academics and Professionals	**30** Partners (Academia, Industry, Public Authorities)	**6500+** Certification Infrastructure Lines of Code
13 Quantum Trainings	**450+** Likes, Comments, Shares	**130** Quantum Training Hours	**10+** Scientific Publications	**164** Certifications Awarded
15+ International Talks Given	**1** Quantum Book Published	**13** Open-Source Repositories	**19** Quantum HUBs	**42** Quantum Training Teachers
150+ Students at the Hackathon	**6** QKD Metropolitan Networks	**80+** Social Media Posts	**7** National Workshops	**19000+** Impressions on LinkedIn
900+ Diplomas of Participation Awarded	**41** Mentors and Juries at the Quantum Hackathon	**2000+** Messages Exchanged on Discord at the Hackathon	**1** International Policy for EuroQCI Scalability	

It is becoming increasingly clear that the software aspect has become the next obstacle against large-scale adoption and utility of QKD. The software has **critical effects across multiple layers: applications, interoperability, governance, infrastructure optimization**, and more. As QKD equipment continues to bear high costs in order to achieve unconditional security, lack of complementary software able to leverage and extend the unconditional security to the end user over the entire system may represent a drawback. **POLITEHNICA Bucharest's software releases (some open-sourced), ranging from end-user applications to infrastructure, have shown that top-tier security can be achieved in practice in ID Quantique QKD networks**.



Representatives of POLITEHNICA Bucharest, the coordinator of RoNaQCI, have declared **they will continue the fruitful collaboration with ID Quantique for further expanding of the infrastructure, building of innovative products, and developing of vital QKD software**.

December 2025

Quantum Team @ POLITEHNICA Bucharest
https://quantum.upb.ro